WHAT IS CLAIMED IS :

1. Apparatus for authenticating that certain information has been sent by a sender via a dispatcher to a recipient, the apparatus comprising:

means for providing a set A comprising a plurality of information elements a1,...,an, said information element a1 comprising the contents of said dispatched information, and said one or more information elements a2,...,an comprising dispatch-related information and comprise at least the following elements:

a2 - a time indication associated with said dispatch; and

a3 - information describing the destination of said dispatch,

and wherein at least one of said information elements is provided in a manner that is resistant or indicative of tamper attempts by said sender;

means for associating said dispatch-related information with said element a1 by generating authentication--information, in particular comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

means for securing at least part of said authentication-information against undetected tamper attempts of at least said sender.

2. Apparatus according to claim 1, wherein said element a2 comprise at least one element of the group comprising the date associated with said dispatch, and the time associated with said dispatch.

3. Apparatus according to any of claims 1 or 2, wherein said dispatch-related information comprise at least one element of the group comprising the following elements: a completion indication associated with said dispatch, the number of pages dispatched, page number, an indication of identification associated with said sender, said dispatch duration, integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said apparatus, a heading message, and a trailing message.

4. Apparatus according to any of claims 1 to 3, wherein said dispatched information has a form selected from the group comprising the following forms: a paper document and electronic information.

5. Apparatus according to any of claims 1 to 4, wherein the elements of said authentication-information and of said set A have a form selected from the group comprising the following forms: a paper document and electronic information, and where each of said elements can have different form.

6. Apparatus according to any of claims 1 to 5, wherein the information originally provided by said sender for dispatch has a form selected from a group comprising the following forms: a paper document and electronic information.

7. Apparatus according to any of claims 1 to 6, wherein said element a1 is provided by means comprising at least one of the following means: a communication network, a scanning device, a copier, a dispatcher, and a computer.

8. Apparatus according to any of claims 1 to 7, wherein said dispatcher comprise at least one element of the following group: a facsimile machine, a modem, a net-

work interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a dispatching service.

9. Apparatus according to claim 8, wherein said dispatching service comprise at least one element of the following group: a courier service, the registered mail service of the post office, and a message transmission forwarding service.

10. Apparatus according to any of claims 1 to 9, comprising means for providing said dispatched information to said dispatcher.

11. Apparatus according to any of claims 1 to 10, and comprising at least part of said dispatcher.

12. Apparatus according to any of claims claim 1 to 11, comprising means for preparing at least one element of the group comprising the elements of said set A, and said dispatched information.

13. Apparatus according to any of claims 1 to 12, wherein said element a3 comprise at least one element of the group comprising an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

14. Apparatus according any of claims 1 to 13, wherein at least part of said apparatus is resistant or indicative of tamper attempts by at least said sender.

15. Apparatus according to any of claims 1 to 14, comprising means for providing at least part of said authentication-information to an interested party.

16. Apparatus according to claim 15, wherein said interested party comprise at least one element of the following group: said sender, said recipient, an arbitrator, and a legal authority.

17. Apparatus according to any of claims 1 to 16, comprising means for storing at least part of said authentication-information.

18. Apparatus according to any of claims 1 to 17, comprising means for generating a new set B, said set B comprising one or more information elements b1,...,bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprise a digital representation of at least one element of said set A, and where said functions Fi can be different.

19. Apparatus according to claim 18, wherein at least one element of said authentication-information comprise a representation of at least part of said new set B.

20. Apparatus according to any of claims 1 to 19, wherein said set A comprise a link information element, and wherein said authentication-information comprise at least one element which comprise a representation of at least said link element.

21. Apparatus according to any of claims 18 to 20, wherein said function Fi has the property that it is substantially difficult to find a set S' comprising at least one information element, said set S' being different from said subset Si and yet can be used instead, such that applying said function Fi to said set S' will yield said element bi, i.e., such that Fi(S')=bi.

22. Apparatus according to any of claims 18 to 21, wherein said function Fi comprise one or more functions.

23. Apparatus according to any of claims 18 to 22, wherein at least one member of the group comprising the following members: said function Fi, and at least one information element of said new set B, is unknown at least to said sender.

24. Apparatus according to any of claims 1 to 23, comprising means for verifying the authenticity of an information element purported to match a corresponding element of said set A, said verification means comprising:

means for comparing a representation of said purported information element with a representation of at least part of said authentication-information which comprise a representation of at least said corresponding element of said set A to determine if they match.

25. Apparatus according to any of claims 18 to 24, comprising means for verifying the authenticity of a set Si' comprising one or more information elements which are purported to match the corresponding elements of said subset Si, said verification means comprising:

means for generating a new information element bi' comprising a representation of said set Si' which is expressive as said function Fi of the elements of said set Si'; and

means for comparing a representation of said element bi' with a representation of said element bi to determine if they match.

26. Apparatus according to any of claims 18 to 25, wherein said function Fi comprise at least one reversible function, comprising means for generating a set C which comprise one or more information elements c1,...,ck, where said set C is expressive as a function I of at least part

of said information element bi, and said function I comprising the inverse function of at least one of said reversible functions.

27. A method for authenticating that certain information has been sent by a sender via a dispatcher to a recipient, comprising the steps of:

providing a set A comprising a plurality of information elements a1,...,an, said information element a1 comprising the contents of said dispatched information, and said one or more information elements a2,...,an comprising dispatch-related information and comprise at least the following elements:

a2 - a time indication associated with said dispatch; and

a3 - information describing the destination of said dispatch,

and wherein at least one of said information elements is provided in a manner that is resistant or indicative of tamper attempts by said sender;

associating said dispatch-related information with said element a1 by generating authentication-information, in particular comprising a representation of at least said elements a1, a2 and a3, said representation comprising a set of one or more elements, each comprising a representation of one or more elements of said set A; and

securing at least part of said authentication-information against undetected tamper attempts of at least said sender.

28. A method according to claim 27, wherein at least part of the activities described by said steps is performed by an authenticator, said authenticator comprising at least one element of the following group: a party other than said sender, said dispatcher, a device, and any combination thereof.

29. A method according to any of claims 27 or 28, wherein said dispatch-related information comprise at least one element of the group comprising the following elements: a completion indication associated with said dispatch, the number of pages dispatched, page number, an indication of identification associated with said sender, said dispatch duration, integrity information, an indication of dispatch identification associated with said dispatch, an indication of identification associated with said authenticator, a heading message, and a trailing message.

30. A method according to any of claims 27 to 29, wherein said dispatched information has a form selected from the group comprising the following forms: a paper document and electronic information.

31. A method according to any of claims 27 to 30, wherein the elements of said authentication-information and of said set A have a form selected from the group comprising the following forms: a paper document and electronic information, and where each of said elements can have different form.

32. A method according to any of claims 27 to 31, wherein the information originally provided by said sender for dispatch has a form selected from a group comprising the following forms: a paper document and electronic information.

33. A method according to any of claims 27 to 32, wherein said element a1 is provided by means comprising at least one of the following means: a communication network, a scanning device, a copier, a dispatcher, and a computer.

34. A method according to any of claims 27 to 33, wherein said dispatcher comprise at least one element of the following group: a facsimile machine, a modem, a net-

work interface card (NIC), a computer, a communication line, a communication network, an E-Mail system, an EDI system, and a dispatching service.

35. A method according to claim 34, wherein said dispatching service comprise at least one element of the following group: a courier service, the registered mail service of the post office, and a message transmission forwarding service.

36. A method according to any of claims 27 to 35, comprising the step of providing said dispatched information to said dispatcher.

37. A method according to any of claims 27 to 36, wherein said element a2 comprise at least one element of the group comprising the date associated with said dispatch, and the time associated with said dispatch.

38. A method according to any of claims 27 to 37, comprising the step of preparing at least one element of the group comprising the elements of said set A, and said dispatched information.

39. A method according to any of claims 27 to 38, wherein said element a3 comprise at least one element of the group comprising an address associated with said dispatch, an address associated with said recipient, and an indication of identification associated with said recipient.

40. A method according any of claims 27 to 39, comprising the step of dispatching said information to said recipient.

41. A method according to any of claims 27 to 40, comprising the step of providing a representation of at

least part of said authentication-information to an interested party.

42. A method according to claim 41, wherein said interested party comprise at least one element of the following group: said sender, said recipient, an arbitrator, and a legal authority.

43. A method according to any of claims 27 to 42, comprising the step of storing at least part of said authentication-information in a storage device.

44. A method according to any of claims 28 or 43, wherein at least part of said device is resistant or indicative of tamper attempts by at least said sender.

45. A method according to any of claims 27 to 44, comprising the step of generating a new set B, said set B comprising one or more information elements b1,...,bm, each element bi comprising a representation of a subset Si, said representation being expressive as a function Fi of the elements of said subset Si, where said subset Si comprise a digital representation of at least one element of said set A, and where said functions Fi can be different.

46. A method according to claim 45, wherein at least one element of said authentication-information comprise a representation of at least part of said new set B.

47. A method according to any of claims 27 to 46, wherein said set A comprise a link information element, and wherein said authentication-information comprise at least one element which comprise a representation of at least said link element.

48. A method according to any of claims 45 to 47, wherein said function Fi has the property that it is sub-

stantially difficult to find a set S' comprising at least one information element, said set S' being different from said subset Si and yet can be used instead, such that applying said function Fi to said set S' will yield said element bi, i.e., such that Fi(S')=bi.

49. A method according to any of claims 45 to 48, wherein said function Fi comprise one or more functions.

50. A method according to any of claims 45 to 49, wherein at least one member of the group comprising the following members: said function Fi, and at least one information element of said new set B, is unknown at least to said sender.

51. A method according to any of claims 27 to 50, comprising the step of verifying the authenticity of an information element purported to match a corresponding element of said set A, said verification step comprising the step of:

comparing a representation of said purported information element with a representation of at least part of said authentication-information which comprise a representation of at least said corresponding element of said set A to determine if they match.

52. A method according to any of claims 45 to 51, comprising the step of verifying the authenticity of a set Si' comprising one or more information elements which are purported to match the corresponding elements of said subset Si, said verification step comprising the steps of:

generating a new information element bi' comprising a representation of said set Si' which is expressive as said function Fi of the elements of said set Si'; and

comparing a representation of said element bi' with a representation of said element bi to determine if they match.

53. A method according to any of claims 45 to 52, wherein said function Fi comprise at least one reversible function, comprising the step of generating a set C which comprise one or more information elements c1,...,ck, where said set C is expressive as a function I of at least part of said information element bi, and said function I comprising the inverse function of at least one of said reversible functions.

54. Apparatus according to any of claims 18 to 26, wherein said new set B comprises a verifiable digital signature of said subset Si.

55. Apparatus according to claim 54, comprising a corresponding verification means for said verifiable digital signature, for authenticating at least one of the following: at least one element of said subset Si, and the originator of said digital signature.

56. Apparatus according to any of claims 54 or 55, wherein said digital signature is generated according to a scheme selected from the group comprising: secret-key (symmetric) cryptosystem, and public-key cryptosystem.

57. Apparatus according to any of claims 1 to 26, or 54 to 56, comprising means for time-stamping at least one element of the group comprising the elements of said authentication-information and the elements of said set A, according to a Time Stamping Service scheme.

58. Apparatus according to any of claims 1 to 26, or 54 to 57, comprising means for authenticating the identity of at least one member of the group comprising: said sender, said recipient, an agent of said sender, and an agent of said recipient.

59. A method according to any of claims 45 to 53, wherein said new set B comprises a verifiable digital signature of said subset Si.

60. A method according to claim 59, comprising a corresponding verification step for said verifiable digital signature, for authenticating at least one of the following: at least one element of said subset Si, and the originator of said digital signature.

61. A method according to any of claims 59 or 60, wherein said digital signature is generated according to a scheme selected from the group comprising: secret-key (symmetric) cryptosystem, and public-key cryptosystem.

62. A method according to any of claims 27 to 53, or 59 to 61, comprising the step of time-stamping at least one element of the group comprising the elements of said authentication-information and the elements of said set A, according to a Time Stamping Service scheme.

63. A method according to any of claims 27 to 53, or 59 to 62, comprising the step of authenticating the identity of at least one member of the group comprising: said sender, said recipient, an agent of said sender, and an agent of said recipient.

add A'

add B'